1. A dynamic file access control and management system configured to access one or more content sources including a set of files, said system comprising:

A a proxy system linked to said one or more content sources, said proxy system comprising an access control module configured to selectively obtain a file from said content sources as a function of an authorization of a user requesting said file and a set of access policies;

B. a rights management module configured to generate a set of usage rights associated with said file as a function of a set of predefined usage policies associated with said file for said user;

C. at least one client device having a client module configured to interface to a client operating system, said client module configured to selectively inhibit operating system functions with respect to said file as a function of said usage rights; and

D. one or more communication means, via which said file and said usage rights are provided to said client device.

2. The system according to claim 1, wherein said file and said usage rights are provided to said client device via different communication means.

3. The system according to claim 1, wherein said files are static files.

4. The system according to claim 1, wherein said files are dynamic files.

A1

5. (Amended) The system according to claim 1, wherein said communication means includes a secure transform configured to encrypt and encapsulate said file into a message as a function of a session ID and said client is configured to extract said file from said message.

6. The system according to claim 1, wherein said proxy system further includes a user interface, configured to facilitate creation and editing of said access policies and said usage policies and association of said access policies and said usage policies with said files.

A2

7. (Amended) The system as in claim 1, wherein said client device is a device from a group comprising:

1) a personal computer;
2) a workstation;
3) a personal digital assistant;
4) an e-mail device;
5) a cellular telephone;
6) a Web enabled appliance; and
7) a server.

8. The system of claim 1, wherein said proxy system and at least one of said content sources are hosted on the same computing device.

A3

9. (Amended) A method of dynamic file access control and management comprising:

A. to each of a set of files accessible from a set of content sources by a proxy system, correlating one or more user and/or client device identifications and defining a set of usage policies, wherein for a given file said usage policies relate to selectively enabling or disabling operations associated with said file;

B. by said proxy system, generating a set of usage rights associated with a target file as a function of a set of usage policies associated with said target file and a user or client device identification;

C. communicating said target file and said usage rights to a client device associated with said identification; and

D. using a client module at said client device and configured to interface to a client operating system, selectively inhibiting operating system functions with respect to said target file as a function of said usage rights.

10. (New) The method of claim 9, wherein in step C, said communicating is accomplished by communicating said target file and said usage rights to said client device via different communication means.

A4

11. (New) The method of claim 9, wherein said set of files include static files.

12. (New) The method of claim 9, wherein said set of files include dynamic files.

13. (New) The method of claim 9, wherein said communicating is accomplished using a communication means that includes a secure transform, including encrypting and encapsulating said target file into a message as a function of a session ID and said client device is configured to extract said target file from said message.

14. (New) The method of claim 9, wherein said proxy system further includes a user interface and step A include creating and/or editing said access policies and said usage policies and associating said access policies and said usage policies with said set of files using said user interface.

15. (New) The method of claim 9, wherein said client device is a device from a group comprising:

1) a personal computer;

2) a workstation;

3) a personal digital assistant;

Cont A4

4) an e-mail device;

5) a cellular telephone;

6) a Web enabled appliance; and

7) a server.

16. (New) The method of claim 9, further comprising hosting said proxy system and at least one content source on the same computing device.